ECLT5820 Distributed and Mobile Systems

Assignment 1 (Topics 1-4)

Due – 11:59pm, 11th Oct. 2021 (Monday)

Please send a pdf file to eclt5820@cse.cuhk.edu.hk with Email title and file name "ECLT5820 Asg#1, Your name, Your student ID".

Q1 (**20 points**) Suppose you are building a large-scale shopping website. In order to provide good service and user experience, what characteristics will you consider in your system? For example, the website should be accessible using different devices, safe for customers to use, and robust when failures happen. Try to illustrate at least five characteristics with explanations.

Q2 (**20 points**) Please explain your choice about whether we should use TCP protocol or UDP protocol to implement the following application-level protocols.

1) File transfer (e.g., FTP)
2) Information browsing (e.g., HTTP)
3) Domain name system (DNS)
4) Remote procedure call (RPC)
5) Streaming media (e.g., Real-time Transport Protocol)

Is UDP more reliable than TCP? Please justify your answer with details.

Q3 (**20 points**) Suppose you are an email user. When you are using an email system (e.g., login, sending email, or receiving email), what are some potential passive attacks and active attacks you might suffer? Try to identify at least four of them with examples. Design proper security mechanisms to handle (either by prevention or detection) these attacks.

Q4 (**15 points**) Consider the RSA encryption algorithm. Please write down your computation details.

1) p=5, q=11, and e=7, what is the corresponding public key and a possible private key?
2) Try to encrypt '2' with the public key and decrypt '15' with the private key.
3) Assuming Alice has her key pair, denoted as PUBKEY(Alice) and PRIKEY(Alice), and Bob has his key pair, denoted as PUBKEY(Bob) and PRIKEY(Bob). Please design a security mechanism for the following application scenario: Alice sends to Bob an invitation message, and Bob replies with a confirmation. What security features can the mechanism provide? Is there any potential vulnerability of your design? Please explain.

Q5 (**25 points**) Please answer the following two questions.

1) Name three advantages and three disadvantages of distributed systems over centralized ones.
2) What are Naming service and Trading service? What are the differences between them? What are the pros and cons of them when comparing with each other?